Empowered by Innovation NEC

ディジタル認証装置

CK-Guard Ⅳ

CK-Guard Ⅳは、ディジタル証明書等を利用する各種セキュリティシステムにおいて、暗号鍵（公開鍵・秘密鍵）の生成および保管を行うタンパフリーな専用ハードウェア装置です。また、生成した秘密鍵によるディジタル署名、復号機能も有しています。なお、本装置を使用するにあたっては、上位装置としてサーバ（SecureWare/秘密鍵装置マネージャ）との接続が必要です

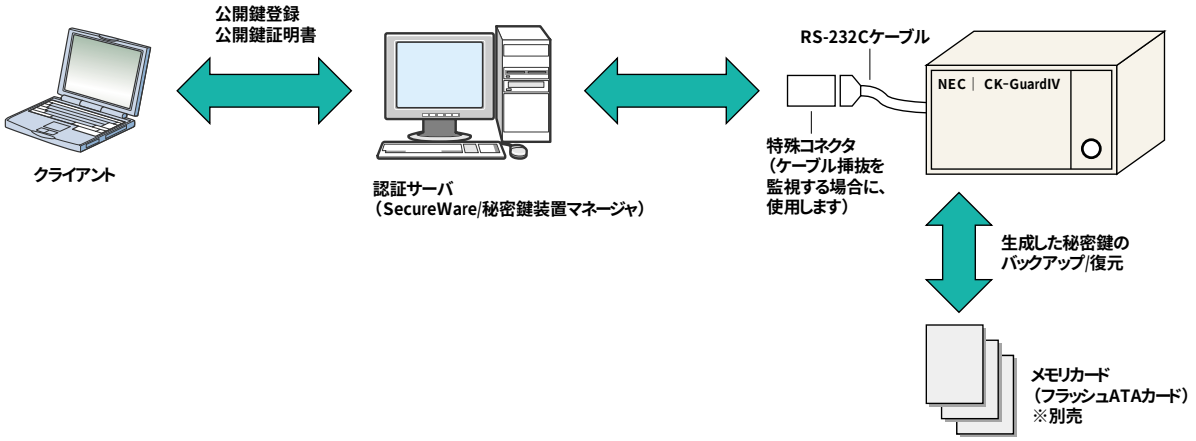
外観は変更になる場合があります。

■主な特長

サーバ（SecureWare/秘密鍵装置マネージャ）と接続して使用することで、Rivest、Shamir、Adlemanにより開発された公開鍵暗号方式において以下の機能を提供します。

- 秘密鍵/公開鍵の生成機能
- ディジタル署名機能（認証機能）
- 秘密鍵による復号機能
- タンパフリー構造の採用により、装置内部に保管した秘密鍵を強力に保護
  - ・One Wrap Around構造により不正解体を防止
  - ・複製困難な2つの物理的鍵（電子錠）を内蔵
  - ・物理的不正アクセスの検出
- トリプルDES/AES暗号による秘密鍵の分散バックアップ機能
  - ・分散枚数＞復元枚数となるシークレットキーシェアリング機能もサポート
- 乱数生成機能
- DES暗号 / 復号機能
- ログ出力による装置不正操作の通知機能

■アプリケーション例



■主な仕様

項目		内容
外部インターフェイス	物理的条件	ITU-T勧告　V.24/V.28並びにJIS-X-5101に準拠
	データタイプ	調歩同期式
	キャラクタ長	8bit/パリティ無し/ストップビット1bit
	データ速度	9600/19200/38400/57600/115200 bps
	フロー制御	RS-CS制御
	通信プロトコル	独自方式
フィジカルセキュリティ	二重化錠による保護 ①保護用錠（錠A） ②操作用錠（錠B）	
	One Wrap Around構造	
暗号方式	①非対称鍵暗号方式（*注） 鍵長：512/768/1024/1280/1536/1792/2048 bit 鍵種別：①署名 ②復号 鍵生成数：15ヶ（最大） ②対称鍵暗号方式（DES） 鍵長：56 bit 鍵生成数：10ヶ（最大） ③対称鍵暗号方式（トリプルDES） 鍵長：112 bit ④対称鍵暗号方式（AES）	
鍵のバックアップ	メモリカード（フラッシュATAカード）へのバックアップ ①トリプルDES（鍵長112 bit）、またはAES(鍵長 128/192/256 bit)にて暗号化（オプション） ②暗号使用時：1枚のメモリカードに格納、または2～10枚のメモリカードに分散して格納 暗号未使用時：3～10枚のメモリカードに分散して格納	
キーの保護	①バッテリバックアップ ②不正時の暗号鍵自動消去	
警報機能	ブザー音、LED	
時計	西暦 / 月 / 日 / 時 / 分 / 秒	
使用電源	AC100V±10%　50/60Hz	
消費電力	約40VA	
温度・湿度	10～40℃・85%以下（但し、結露しないこと）	
外形寸法	315(W)×130(H)×395(D)mm ※ 高さはゴム足：14mm含まず。 ※ 奥行きはSTAPLE（背面部取手）：22mm含まず。	
質量	約13kg	
FG端子ネジ	M4ネジ	
電源コード長	約3m	
規格	VCCIクラスB	
セキュリティ機能	FIPS140-2レベル3相当	

（注）Rivest/Shamir/Adlemanにより開発された公開鍵暗号方式

⚠ 安全に関するご注意　★本製品の設置・接続・使用に際しましては、取扱説明書などに記載されております注意事項や禁止事項をあらかじめ熟読のうえ、必ずお守りください。

●本カタログ中の社名、商品名は各社の商標または登録商標です。
●このカタログに記載された仕様、デザインなどは、予告なしに変更することがあります。

お問い合わせは、下記のNECへ

NECブロードバンドネットワーク事業本部
NECマグナスコミュニケーションズ
http://www.nec.co.jp/access/

日本電気株式会社　〒108-8001 東京都港区芝五丁目7-1（NEC本社ビル）
NECマグナスコミュニケーションズ株式会社　〒108-0073 東京都港区三田一丁目4-28（三田国際ビル）